IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	:	
Masayoshi NISHITANI et al.	:	
Serial No.	:	Art Unit:
Filed: September 15, 2003	:	Examiner:
For: SYSTEM FOR TRANSMITTING AND RECEIVING ENCRYPTED INFORMATION	:	Atty Docket: 0124/0013

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Attached hereto please find a certified copy of applicants' Japanese application No. 2002-341590 filed November 26, 2002.

Applicants request the benefit of said November 26, 2002 filing date for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, Reg. No. 31,730
Law Offices of Louis Woo
717 North Fayette Street
Alexandria, Virginia 22314
Phone: (703) 299-4090

Date: Sept 15 2003

VH1105

日　本　国　特　許　庁
JAPAN　PATENT　OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application:　２００２年１１月２６日

出願番号
Application Number:　特願２００２－３４１５９０

[ST.10/C]:　[ＪＰ２００２－３４１５９０]

出願人
Applicant(s):　日本ビクター株式会社

２００３年　６月３０日

特許庁長官
Commissioner,
Japan Patent Office　太田信一郎

出証番号　出証特２００３－３０５１４１５

【書類名】　特許願

【整理番号】　41400916

【提出日】　平成14年11月26日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/00

G09C　5/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　西谷　勝義

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　上田　健二朗

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　菅原　隆幸

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代表者】　寺田　雅彦

【代理人】

【識別番号】　100089956

【弁理士】

【氏名又は名称】　永井　利和

【電話番号】　03(3707)5055

【手数料の表示】

【予納台帳番号】　004813

【納付金額】　　21,000円

【提出物件の目録】

【物件名】　　明細書　1

【物件名】　　図面　1

【物件名】　　要約書　1

【包括委任状番号】　9200897

【プルーフの要否】　　要

【書類名】　明細書

【発明の名称】　暗号情報の送受信システム、送受信方法及び暗号情報埋め込み用プログラム

【特許請求の範囲】

【請求項１】　暗号情報記録部と暗号情報再生部が伝送路を介して配置せしめられ、前記暗号情報記録部側からディジタル・コンテンツに暗号情報を埋め込んだディジタル信号を前記暗号情報再生部へ送信し、前記ディジタル信号を受信した前記暗号情報再生部側で前記暗号情報を再生する暗号情報の送受信システムにおいて、

前記暗号情報記録部が、

前記ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割するデータ分割手段と、

前記データブロック毎にそのブロック内のディジタル信号の統計量を算出するパラメータ算出手段と、

埋め込み情報を暗号化して暗号情報として出力する暗号変換手段と、

前記暗号情報と前記統計量に基づいて、前記データブロック内のディジタル信号の統計量を変更するための加減算量を算出する加減算量算出手段と、

擬似乱数テーブルと、

前記擬似乱数テーブルから乱数を読出し、前記乱数の値に前記加減算量を加算して新たな擬似乱数信号を作成する埋め込み乱数作成手段と、

前記データブロック内のディジタル信号に前記擬似乱数信号を加算する加算手段とを具備し、

前記暗号情報再生部が、

伝送されたディジタル信号を前記暗号情報記録部側のデータ分割手段による分割処理に対応したデータブロックである再生側データブロックに分割する再生側データ分割手段と、

前記再生側データブロック毎に、そのブロック内のディジタル信号における前記暗号情報記録部側のパラメータ算出手段で算出する統計量と同じ統計量を算出する再生側パラメータ算出手段と、

その算出された前記再生側データブロックの統計量に基づき、前記暗号化情報記録部側の加減算量算出手段での統計量変更処理に応じて前記暗号情報を判定し、その暗号情報を伝送された前記ディジタル信号から抽出する判定・抽出手段と、

前記暗号情報記録部側の暗号変換手段と逆のアルゴリズムで、前記判定・抽出手段で抽出された暗号情報を元の埋め込み情報に復元する暗号逆変換手段とを具備した

ことを特徴とする暗号情報の送受信システム。

【請求項２】　暗号情報記録部と暗号情報再生部が伝送路を介して配置せしめられ、前記暗号情報記録部側からディジタル・コンテンツに暗号情報を埋め込んだディジタル信号を前記暗号情報再生部へ送信し、前記ディジタル信号を受信した前記暗号情報再生部側で前記暗号情報を再生する暗号情報の送受信方法において、

前記暗号情報記録部が、

前記ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割するデータ分割手順と、

前記データブロック毎にそのブロック内のディジタル信号の統計量を算出するパラメータ算出手順と、

埋め込み情報を暗号化して暗号情報として出力する暗号変換手順と、

前記暗号情報と前記統計量に基づいて、前記データブロック内のディジタル信号の統計量を変更するための加減算量を算出する加減算量算出手順と、

擬似乱数テーブルから乱数を読出し、前記乱数の値に前記加減算量を加算して新たな擬似乱数信号を作成する埋め込み乱数作成手順と、

前記データブロック内のディジタル信号に前記擬似乱数信号を加算する加算手順とを実行し、

前記暗号情報再生部が、

伝送されたディジタル信号を前記暗号情報記録部側のデータ分割手順による分割処理に対応したデータブロックである再生側データブロックに分割する再生側データ分割手順と、

前記再生側データブロック毎に、そのブロック内のディジタル信号における前記暗号情報記録部側のパラメータ算出手順で算出する統計量と同じ統計量を算出する再生側パラメータ算出手順と、

その算出された前記再生側データブロックの統計量に基づき、前記暗号化情報記録部側の加減算量算出手順での統計量変更処理に応じて前記暗号情報を判定し、その暗号情報を伝送された前記ディジタル信号から抽出する判定・抽出手順と、

前記暗号情報記録部側の暗号変換手順と逆のアルゴリズムで、前記判定・抽出手順で抽出された暗号情報を元の埋め込み情報に復元する暗号逆変換手順とを実行する

ことを特徴とする暗号情報の送受信方法。

【請求項３】　暗号情報記録部を構成するコンピュータによりディジタル・コンテンツに暗号情報を埋め込むためのプログラムであって、

前記ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割するデータ分割手順と、

前記データブロック毎にそのブロック内のディジタル信号の統計量を算出するパラメータ算出手順と、

埋め込み情報を暗号化して暗号情報として出力する暗号変換手順と、

前記暗号情報と前記統計量に基づいて、前記データブロック内のディジタル信号の統計量を変更するための加減算量を算出する加減算量算出手順と、

擬似乱数テーブルから乱数を読出し、前記乱数の値に前記加減算量を加算して新たな擬似乱数信号を作成する埋め込み乱数作成手順と、

前記データブロック内のディジタル信号に前記擬似乱数信号を加算する加算手順と

をコンピュータに実行させるものである暗号情報埋め込み用プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像や音楽等のディジタル・コンテンツに暗号情報を付加して伝送

するための暗号情報の送受信システム、送受信方法及び暗号情報埋め込み用プログラムに係り、著作権の証明や侵害の識別、又は隠されたメッセージ等を送信する場合に適用され、より簡単な方式で暗号情報の埋め込みと再生を可能にするための改良に関する。

【０００２】

【従来の技術】

近年、インターネット等の通信回線を介した画像や音楽等のディジタル・コンテンツの流通が益々盛んになっているが、それらコンテンツの不正な複製や改竄を防止するために、コンテンツのディジタル信号に暗号化した電子透かし信号を埋め込んで隠し持たせる各種の方法が提案されている。

例えば、下記の非特許文献１では、電子透かし情報埋め込み方法として、暗号情報をＭＰＥＧ方式により圧縮符号化された符号、特にＤＣＴ係数や、動きベクトル、量子化特性の変更による情報埋め込みについて検討し、ＤＣＴ係数の変更による手法が、編集や圧縮による著作権情報の消し込みに対して耐性の点で優れていることを示唆している。

【０００３】

また、下記の非特許文献２においては、直接拡散方式に従い、ＰＮ系列で画像信号を拡散し、画像に署名情報を合成する方法を提案している。

この提案では、署名を含んだ画像信号を逆拡散すると、署名情報は画像信号全体に拡散し、拡散された信号は非常に弱く、画像信号に対して大きなノイズとはならないために、署名情報を含んだ画像信号が見かけ上は殆ど原画像と変らないことを明らかにし、逆に、署名情報を確認するには、拡散符号で画像信号を拡散することにより、署名情報の信号を検出することとしている。

【０００４】

【非特許文献１】

電子情報通信学会　掲載番号：ＳＣＳＩ’９７－３１Ｇ

タイトル：DCTを用いたデジタル動画像における著作権情報埋め込み方法

著者名：小川宏，中村高雄，高嶋洋一

【非特許文献２】

電子情報通信学会　掲載番号：ＳＣＳＩ’９７－２６Ｂ

タイトル：PN系列による画像への透かし署名法

著者名：大西淳児，岡一博，松井甲子雄

【０００５】

【発明が解決しようとする課題】

しかし、前記の非特許文献１，２の電子透かし埋め込み方法によれば、複雑な信号処理を要し、透かし情報を画像に埋め込んで伝送する際に、画像の変換処理に時間がかかると共に、そのためのハードウェアやソフトウェアの製造コストが高くなるという問題がある。

また、ＤＣＴ等の直交変換を用いて算出された変換係数に対して透かし情報を埋め込むと、簡単な低域通過フィルタでも透かし情報が欠損する恐れがある。

【０００６】

そこで、本発明は、より簡単な装置と手順で暗号情報の埋め込みとその再生を可能にし、前記の問題点を解消した暗号情報の送受信方法、送受信システム及び暗号情報埋め込み用プログラムを提供することを目的として創作された。

【０００７】

【課題を解決するための手段】

第１の発明は、暗号情報記録部と暗号情報再生部が伝送路を介して配置せしめられ、前記暗号情報記録部側からディジタル・コンテンツに暗号情報を埋め込んだディジタル信号を前記暗号情報再生部へ送信し、前記ディジタル信号を受信した前記暗号情報再生部側で前記暗号情報を再生する暗号情報の送受信システムにおいて、前記暗号情報記録部が、前記ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割するデータ分割手段と、前記データブロック毎にそのブロック内のディジタル信号の統計量を算出するパラメータ算出手段と、埋め込み情報を暗号化して暗号情報として出力する暗号変換手段と、前記暗号情報と前記統計量に基づいて、前記データブロック内のディジタル信号の統計量を変更するための加減算量を算出する加減算量算出手段と、擬似乱数テーブルと、前記擬似乱数テーブルから乱数を読出し、前記乱数の値に前記加減算量を加算して新たな擬似乱数信号を作成する埋め込み乱数作成手段と、前記データブ

ロック内のディジタル信号に前記擬似乱数信号を加算する加算手段とを具備し、前記暗号情報再生部が、伝送されたディジタル信号を前記暗号情報記録部側のデータ分割手段による分割処理に対応したデータブロックである再生側データブロックに分割する再生側データ分割手段と、前記再生側データブロック毎に、そのブロック内のディジタル信号における前記暗号情報記録部側のパラメータ算出手段で算出する統計量と同じ統計量を算出する再生側パラメータ算出手段と、その算出された前記再生側データブロックの統計量に基づき、前記暗号化情報記録部側の加減算量算出手段での統計量変更処理に応じて前記暗号情報を判定し、その暗号情報を伝送された前記ディジタル信号から抽出する判定・抽出手段と、前記暗号情報記録部側の暗号変換手段と逆のアルゴリズムで、前記判定・抽出手段で抽出された暗号情報を元の埋め込み情報に復元する暗号逆変換手段とを具備したことを特徴とする暗号情報の送受信システムに係る。

【０００８】

第２の発明は、暗号情報記録部と暗号情報再生部が伝送路を介して配置せしめられ、前記暗号情報記録部側からディジタル・コンテンツに暗号情報を埋め込んだディジタル信号を前記暗号情報再生部へ送信し、前記ディジタル信号を受信した前記暗号情報再生部側で前記暗号情報を再生する暗号情報の送受信方法において、前記暗号情報記録部が、前記ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割するデータ分割手順と、前記データブロック毎にそのブロック内のディジタル信号の統計量を算出するパラメータ算出手順と、埋め込み情報を暗号化して暗号情報として出力する暗号変換手順と、前記暗号情報と前記統計量に基づいて、前記データブロック内のディジタル信号の統計量を変更するための加減算量を算出する加減算量算出手順と、擬似乱数テーブルから乱数を読出し、前記乱数の値に前記加減算量を加算して新たな擬似乱数信号を作成する埋め込み乱数作成手順と、前記データブロック内のディジタル信号に前記擬似乱数信号を加算する加算手順とを実行し、前記暗号情報再生部が、伝送されたディジタル信号を前記暗号情報記録部側のデータ分割手順による分割処理に対応したデータブロックである再生側データブロックに分割する再生側データ分割手順と、前記再生側データブロック毎に、そのブロック内のディジタル信号に

おける前記暗号情報記録部側のパラメータ算出手順で算出する統計量と同じ統計量を算出する再生側パラメータ算出手順と、その算出された前記再生側データブロックの統計量に基づき、前記暗号化情報記録部側の加減算量算出手順での統計量変更処理に応じて前記暗号情報を判定し、その暗号情報を伝送された前記ディジタル信号から抽出する判定・抽出手順と、前記暗号情報記録部側の暗号変換手順と逆のアルゴリズムで、前記判定・抽出手順で抽出された暗号情報を元の埋め込み情報に復元する暗号逆変換手順とを実行することを特徴とする暗号情報の送受信方法に係る。

【０００９】

前記の各発明では、暗号情報記録部が、ディジタル・コンテンツのディジタル信号を所定データ量のデータブロックに分割し、埋め込み情報を暗号化して作成した暗号情報を前記のデータブロック単位の信号に記録して送信する。

ディジタル・コンテンツのディジタル信号に対する暗号情報の埋め込みに際しては、予め、データブロック内のディジタル信号の統計量が求められ、更にその統計量と暗号情報に基づいてデータブロックのディジタル信号の統計量を変更するための加減算量が求められ、擬似乱数テーブルから読み出された乱数の値に前記の加減算量を加算することにより暗号情報を含んだ新たな擬似乱数信号を作成し、それを元のデータブロックのディジタル信号に加算するようにしている。

一方、暗号情報再生部では、暗号情報を含んだディジタル・コンテンツのディジタル信号をデータブロックに分割した後、そのデータブロックの統計量を算出し、統計量に基づいて暗号情報を判定して抽出し、暗号情報記録部の埋め込み乱数作成手順と逆の手順で埋め込み情報を復元する。

但し、暗号情報再生部の各手段又は各手順は暗号情報記録部側の対応する各手段又は各手順と整合性をもっている。

この発明において、「統計量」とは、データブロック単位で求められるディジタル信号の平均値や総和値等の物理量である。

【００１０】

尚、前記の各発明は、ハードウェアだけでなくソフトウェアでも実現でき、ソフトウェアによる場合には、暗号情報記録部と暗号情報再生部をコンピュータで

構成する。

そして、その場合における暗号情報記録部側のプログラムは、第２の発明に係る暗号情報記録部が実行する各手順が記述されたプログラムとされる。

【００１１】

【発明の実施の形態】

以下、本発明の「暗号情報の送受信システム、送受信方法及び暗号情報埋め込み用プログラム」の実施形態を、図面を用いて詳細に説明する。

［実施形態１］

この実施形態では、伝送システムにおける暗号情報の記録部と再生部をハードウェアで構成した場合における、暗号情報の送受信方式を説明する。

先ず、図１は暗号情報の送受信システムの構成を示し、伝送路１を介して暗号情報記録部２と暗号情報再生部３が配置されている。

但し、実際の伝送系では、暗号情報記録部２と伝送路１の間及び暗号情報再生部３と伝送路１の間に、それぞれ通信制御装置が介在することになるが、同図では省略されている。

そして、ここでは、図２に示すような、水平方向の画素数がＷで、垂直方向の画素数がＨである画像情報を伝送する際に、その画像情報を水平方向の画素数がＸで、垂直方向の画素数がＹである画素ブロックＰＢに分割し、その画素ブロック単位で暗号情報を埋め込む場合を例にとって説明することとする。

【００１２】

暗号情報記録部２は、領域分割部２１とパラメータ算出器２２と加減算量算出器２３と暗号変換器２４と埋め込み乱数作成器２５と擬似乱数テーブル２６と加算器２７を備えており、暗号情報の埋め込み処理を次のような動作で実行する。

前記のディジタル画像信号が領域分割器２１へ入力されると、領域分割器２１は、画像信号を図２で示す画素ブロックＰＢ毎に分割し、その画素ブロックＰＢ単位でパラメータ算出器２２へ順次出力する。

【００１３】

パラメータ算出器２２では、各画素ブロックＰＢ毎に各画素の輝度値の総和と平均値を算出し、次の加減算量算出器２３へ出力する。

そして、加減算量算出器２３では、埋め込み情報を暗号変換器２４で暗号化した暗号情報に基づいて、画素ブロックＰＢの輝度の平均値を変更するように、画素ブロックＰＢ内の輝度信号に加減算する輝度総和値を算出する。

【００１４】

ここに、暗号化の簡単な一例としては、埋め込み情報がＡＳＣＩＩ（登録商標）文字であれば、文字は１バイトで表されるため、８個のビットを１ビットずつ順に画素ブロックＰＢに埋め込むようにすればよく、また、後記の暗号情報再生部３の暗号逆変換器３４との整合性がとれることを条件に、ハフマン符号テーブル等のテーブルを用いて符号化したものを１ビットずつ画素ブロックＰＢに埋め込むようにしてもよい。

【００１５】

また、加減算量算出器２３によって画素ブロックＰＢの輝度の平均値を変更する処理は、画像情報に対する暗号情報の埋め込みが如何なる条件でなされるかについての意味付けに相当し、前記の暗号情報記録部２と暗号情報再生部３の間で相互に設定された規則性である。

この実施形態では、埋め込まれる暗号情報のビットが“１”である場合に画素ブロックＰＢの輝度の平均値を偶数とし、暗号情報のビットが“０”である場合に画素ブロックＰＢの輝度の平均値を奇数とするように規則付けられているものとする。

【００１６】

そこで、加減算量算出器２３では、次のような処理を実行する。

今、パラメータ算出器２２から加減算量算出器２３に入力された画素ブロックＰＢの輝度信号の総和ＳＵＭと平均値ＡＶＧを次式で表すこととする。

【数００１】

$$SUM=\sum_{i=1}^{N} Pi \qquad \cdots ①$$

$$AVG=SUM//N \qquad \cdots ②$$

但し、Ｐｉは画素ブロックＰＢ内の画素の輝度値、Ｎは画素ブロックＰＢ内の画素数、演算子//は除算後に小数点以下を四捨五入する演算を表す。

【００１７】

前記のように、埋め込まれる暗号情報のビットが“１”である場合には、平均値ＡＶＧが偶数となるように変更することになる。

従って、ＡＶＧが奇数になった場合には次のような処理が施される。

先ず、ＡＶＧに１を加算した値（ＡＶＧ1）及びＡＶＧから１を減算した値（ＡＶＧ2）を求めておき、次に、画素ブロックＰＢ内の画素数Ｎを乗じて、平均値が次式のＡＶＧ1及びＡＶＧ2となる画像ブロックＰＢ内の輝度値の総和ＳＵＭ1，ＳＵＭ2を求める。

【数００２】

$$SUM1=AVG1\times N,\quad AVG1=AVG+1 \quad \cdots ③$$

$$SUM2=AVG2\times N,\quad AVG2=AVG-1 \quad \cdots ④$$

【００１８】

そして、次式に示すように、画素ブロックＰＢに係る元の輝度信号の輝度値の総和ＳＵＭと③及び④式から算出された輝度値の総和ＳＵＭ1，ＳＵＭ2との絶対値差分δ1及びδ2を求める。

【数００３】

$$\delta 1=|SUM-SUM1| \quad \cdots ⑤$$

$$\delta 2=|SUM-SUM2| \quad \cdots ⑥$$

【００１９】

また、前記の⑤及び⑥式でδ1とδ2が求まると、それらの大小を比較し、絶対値差分が小さい方の平均値（ＡＶＧ1又はＡＶＧ2）を新たにその画素ブロックＰＢの平均値として選択し、選択した新たな平均値の差分値を埋め込み乱数作成器２５へ出力する。

即ち、ＡＶＧ1が選択された場合には差分値Δ＝ＳＵＭ1－ＳＵＭを、ＡＶＧ2が選択された場合には差分値Δ＝ＳＵＭ2－ＳＵＭを埋め込み乱数作成器２５へ出力する。

【００２０】

ここで、絶対値差分が小さくなる方の平均値を選択するようにしたのは、後記の加算器２７において前記の差分値Δが画素ブロックＰＢ内の画素の加減算に反映されることから、伝送先で画像情報を再生した際に画素ブロック間での表示画像の相違が目立つ等の画質劣化を極力抑制するためである。

尤も、画質劣化が微小であって、ハードウェアの制約条件等からデータ処理数を減らすような場合には、例えば、常に平均値ＡＶＧに１を加算した値を変更後の平均値として選択し、③式によって輝度値の総和ＳＵＭ1を求め、差分値Δ＝ＳＵＭ1－ＳＵＭを埋め込み乱数作成器２５へ出力するようにしてもよい。

【００２１】

一方、画素ブロックＰＢの輝度の平均値ＡＶＧが偶数であった場合には、上記の規則付けに合致して平均値の変更処理を施す必要がないため、埋め込み乱数作成器２５に対して差分値Δ＝０を出力する。

尤も、伝送先において埋め込み情報を検出する際の精度を向上させる観点からみれば、画素ブロックＰＢ内の輝度値の総和が前記の平均値ＡＶＧに画素総数Ｎを乗じた値になるように調整してもよい。

その場合には、画素ブロックＰＢ内の輝度値の総和を次式で求め、

【数００４】

$$SUM3 = AVG \times N \qquad \cdots ⑦$$

元の画素ブロックＰＢの輝度信号の総和ＳＵＭと⑦式の総和ＳＵＭ3との差分値Δ＝ＳＵＭ3－ＳＵＭを求めて埋め込み乱数作成器２５へ出力させることになる。

【００２２】

以上に、埋め込まれる暗号情報のビットが“１”である場合について説明したが、埋め込まれる暗号情報のビットが“０”である場合については、上記の規則性に基づいて画素ブロックＰＢの輝度の平均値を奇数とするように、画素ブロックＰＢの輝度の平均値と総和を用いて前記と同様のアルゴリズムで差分値Δを求め、それを埋め込み乱数作成器２５へ出力させる。

【００２３】

次に、埋め込み乱数作成器２５では、加減算量算出器２３で求めた差分値Δ（加減算量）を用いて、画素ブロックＰＢの各画素に加算するための乱数を作成する。

先ず、擬似乱数テーブル２６を読み出して内部メモリにセーブする。

擬似乱数テーブル２６は予め乱数を発生させて作成したものであり、乱数の平均値が０であって、各乱数の値が整数になっている。

ここでは、説明を簡単にするために、擬似乱数テーブル２６の乱数は画素ブロックＰＢの画素数と同数だけ用意されているものとする。

【００２４】

埋め込み乱数作成器２５は、加減算量算出器２３から得られている前記の差分値Δに応じて擬似乱数テーブル２６の値を変更する。

例えば、差分値Δが正の値である場合には、擬似乱数テーブル２６の中で値の絶対値が小さい方から順に（即ち、先ず０の箇所、±１の箇所、±２の箇所…の順に）、差分値Δの値分だけ乱数の値を１増加させる。

また、逆に、差分値Δが負の値である場合には、同様の条件で擬似乱数テーブル２６の中で値の絶対値が小さい方から順に（即ち、先ず０の箇所、±１の箇所、±２の箇所…の順に）、差分値Δの絶対値分だけ乱数の値を１減少させる。

そして、このようにして作成された擬似乱数は加算器２７へ出力される。

【００２５】

加算器２７では、前記の擬似乱数と本来の画素ブロックＰＢの信号とを画素単位で加算する。

擬似乱数は元々の平均値が０であったものに、加減算量算出器２３において埋め込み情報のビットが“０”であるか“１”であるかに対応させて算出した差分値Δに基づいて前記の加減算を施したものであるため、加算後の画素ブロックＰＢの輝度の平均値は埋め込み情報のビットに応じた値に変更され、また、画素ブロックＰＢ内の各画素の輝度値も埋め込み情報のビットに応じて変更されていることになる。

【００２６】

暗号情報記録部２は、以上のようにして画像情報に埋め込み情報を暗号情報と

して含ませたディジタル画像信号を加算器２７から出力させるが、その出力信号は伝送路１を介して暗号情報再生部３側へ伝送される。

【００２７】

暗号情報再生部３では、先ず、伝送されたディジタル画像信号を領域分割器３１で画素ブロックＰＢ毎に分割する。

即ち、その領域分割器３１は、暗号情報記録部２側の領域分割器２１と整合性を有しており、同様の手順で同サイズの画素ブロックＰＢに分割して、以降の暗号情報再生処理を画素ブロックＰＢ単位で実行できるようにする。

【００２８】

領域分割器３１は各画素ブロックＰＢをパラメータ算出器３２へ出力するが、パラメータ算出器３２では、暗号情報記録部２側のパラメータ算出器２２と同様の手順で、入力された画素ブロックＰＢ毎に画素の輝度値の平均値を算出し、それを判定・抽出器３３へ出力する。

【００２９】

判定・抽出器３３では、画素ブロックＰＢの画素の輝度値の平均値が偶数の場合には暗号情報のビットとして“１”を出力し、逆に奇数の場合には“０”を出力する。

そして、判定・抽出器３３が出力するビット列は暗号逆変換器３４へ入力されるが、暗号逆変換器３４は暗号情報記録部２側の暗号変換器２４の暗号作成アルゴリズムと逆のアルゴリズムで前記のビット列から埋め込み情報を求める。

【００３０】

以上に、本実施形態の暗号情報記録部２と暗号情報再生部３の動作を説明したが、個別の機能部分については次のような変形例も採用できる。

（１）　前記の実施形態では、埋め込み乱数作成器２５で用いる擬似乱数テーブル２６の乱数が画素ブロックＰＢの画素数と同数だけ用意されていることとしたが、ハードウェアのメモリに制約がある等の条件下では、例えば、画素ブロックＰＢの数分の１のサイズの擬似乱数テーブルを用い、そのテーブルを画素ブロックＰＢ内で繰り返して使用するようにしてもよい。

その場合、画素ブロックＰＢに加減算する加減算量を擬似乱数テーブルの使用

回数分で割って分配し、その分配量に応じて各擬似乱数テーブルの値を変更する。

ところで、前記のように繰り返して同一の擬似乱数テーブルを使用すると、画素ブロックＰＢの中にパターン模様が見えてしまうことがある。

その問題に対しては、画素ブロックＰＢに加減算量を加減算する時に、擬似乱数テーブルの読出し開始位置を、加減算を開始する画素ブロックの番号や画素の位置等を利用してランダムに変更することで対処できる。

【００３１】

（２）　前記の実施形態では、暗号情報記録部２の領域分割部２１及び暗号情報再生部３の領域分割部３１以降の処理過程を画素ブロックＰＢ単位で行うようにしているが、埋め込み情報の暗号化ビット数によっては画像情報の全ての画素ブロックＰＢを用いる必要はなく、前記ビット数分の処理を行えば終了とみなしてもよい。

また、逆に、画像情報の画像ブロックＰＢの数が暗号化ビット数より２倍以上大きい場合には、暗号化ビット列を繰り返して埋め込むようにしてもよく、その場合には、伝送路１において混入するノイズ等に対する耐性を高めることができる。

尚、暗号情報再生部３の構成は、暗号情報記録部２との間で整合性をもって埋め込み情報を再生・抽出できれば、どのような再生・抽出方式を採用してもよい。

【００３２】

（３）　前記の実施形態では、暗号情報記録部２と暗号情報再生部３の各領域分割部２１，３１が、単に画像情報を各画像ブロックＰＢに分割する機能のみを担っているが、相互に整合性がとれていることを前提として、領域分割を行う際に暗号化ビットを埋め込み・抽出する領域を判定する機能をそれぞれの各領域分割部２１，３１に含ませてもよい。

【００３３】

（４）　暗号情報記録部２の暗号変換器２４の暗号変換方式についても、前記の実施形態の例だけでなく、各種の方式を採用することができる。

【００３４】

［実施形態２］

前記の実施形態１では暗号情報記録部２と暗号情報再生部３の各機能をハードウェアで実行させるようにしているが、それらはソフトウェア（プログラム）処理で実行させることも可能である。

その場合には、図３に示すように、暗号情報記録部２’と暗号情報再生部３’をマイクロコンピュータ回路で構成し、各マイクロコンピュータ回路のＲＯＭ４１，５１に図１の暗号情報記録部２と暗号情報再生部３の各機能部が実行する動作手順に係るプログラムモジュールを格納しておき、ＣＰＵ４２，５２がそれらのプログラムを順次実行することにより、実施形態１の場合と同様の信号処理を行うことになる。

このシステムによれば、暗号情報記録部２’では、擬似乱数テーブルをＲＯＭ４１に格納しておき、また、埋め込み情報を予め暗号変換プログラムによって暗号化ビット列に変換しておき、そのビット列をＲＡＭ４３に格納しておくことができる。

【００３５】

暗号情報記録部２’におけるデータ処理手順は、図４のフローチャートに示される。

同図から明らかなように、基本的なデータ処理手順は実施形態１において暗号情報記録部２の各機能部が実行する手順と同様であるが、Ｉ/Ｏポート４４を介して入力される画素ブロックＰＢに対する管理をカウンタによって実行している点が相違している。

即ち、画像情報を領域分割して得られる各画素ブロックＰＢに対する、パラメータ値の算出手順（S4）と、暗号情報の各ビットに基づいた画素ブロック内ＰＢの加減算量の算出手順(S5)と、擬似乱数テーブルを加減算量に基づいて変更して埋め込み乱数を作成する手順(S6)と、画素ブロックＰＢ内の各画素の輝度信号に埋め込み乱数を加算する手順(S7)とからなる一連の手順を、カウンタの値を＋１インクリメントしながら管理し、その都度、暗号情報の次のビットが加減算量の算出手順(S5)に適用されるようにしている(S9)。

尚、ステップS8は、図２に示した画像情報全体の画素ブロックＰＢが全て処理されたか否かを判断する手順である。

【００３６】

埋め込み情報を暗号情報として含んだディジタル画像信号はＩ/Ｏポート４４から伝送路１を介して暗号情報再生部３’側へ伝送される。

暗号情報再生部３’におけるデータ処理手順は、図５のフローチャートに示される。

このフローチャートにおける基本的なデータ処理手順も、実施形態１において暗号情報再生部３の各機能部が実行する手順と同様であるが、前記と同様に、Ｉ/Ｏポート５４を介して入力される画素ブロックＰＢに対する管理をカウンタによって実行している点が相違している。

即ち、画像情報を領域分割した後の各画素ブロックＰＢに対する、画素ブロックのパラメータ値を算出する手順(S14)と、パラメータ値に基づいて暗号情報のビットを判定・抽出して出力する手順(S15)をカウンタの値を＋１インクリメントしながら管理している(S17)。

尚、ステップS16は、図２に示した画像情報全体の画素ブロックＰＢが全て処理されたか否かを判断する手順である。

【００３７】

また、この暗号情報再生部３’では、ステップS15で判定・抽出される暗号情報のビットを一旦ＲＡＭ５３にセーブさせ、画像情報全体の画素ブロックＰＢが全て処理された段階で、ＲＡＭ５３にセーブされた暗号化ビット列をＲＯＭ５１の暗号逆変換プログラムによって逆変換することにより埋め込み情報を求めるようにしている(S18)。

【００３８】

尚、図４及び図５のフローチャートでは、画像情報全体の画素ブロックＰＢに暗号情報が含まれていることを前提とした処理手順を示しているが、暗号情報記録部２’と暗号情報再生部３’とで整合性がとれていれば、どのような終了条件を設定してもよい。

例えば、カウンタがカウントする上限値を予め設定しておき、その回数分だけ

の画素ブロックＰＢが処理された段階で終了させるようにしてもよい。

【００３９】

【発明の効果】

本発明の「暗号情報の送受信システム、送受信方法及び暗号情報埋め込み用プログラム」は、以上の構成を有していることにより、次のような効果を奏する。

ディジタル・コンテンツの伝送に際して、分割されたディジタル信号に埋め込む暗号情報に応じて算出された信号の加算量を、擬似乱数を変化させた態様で前記の分割後のディジタル信号に加減算することにより、より簡単な装置と手順で暗号情報の埋め込みとその再生を可能にし、伝送システムの構築に大きなコストをかけることなく、データ処理時間も短い暗号情報の伝送を実現する。

また、信号全体に乱数を加減算しているため、スペクトル拡散と同様の拡散効果が得られ、耐性の強い電子透かし記録及び再生が可能になるという利点もある。

【図面の簡単な説明】

【図１】

本発明の実施形態１（暗号情報記録部と暗号情報再生部をハードウェアで構成した場合）に係る暗号情報の送受信システムの構成図である。

【図２】

画像情報に対する画素ブロックの分割態様を示す概略図である。

【図３】

本発明の実施形態２（暗号情報記録部と暗号情報再生部をソフトウェアで構成した場合）に係る暗号情報の送受信システムの構成図である。

【図４】

暗号情報記録部のデータ処理手順を示すフローチャートである。

【図５】

暗号情報再生部のデータ処理手順を示すフローチャートである。

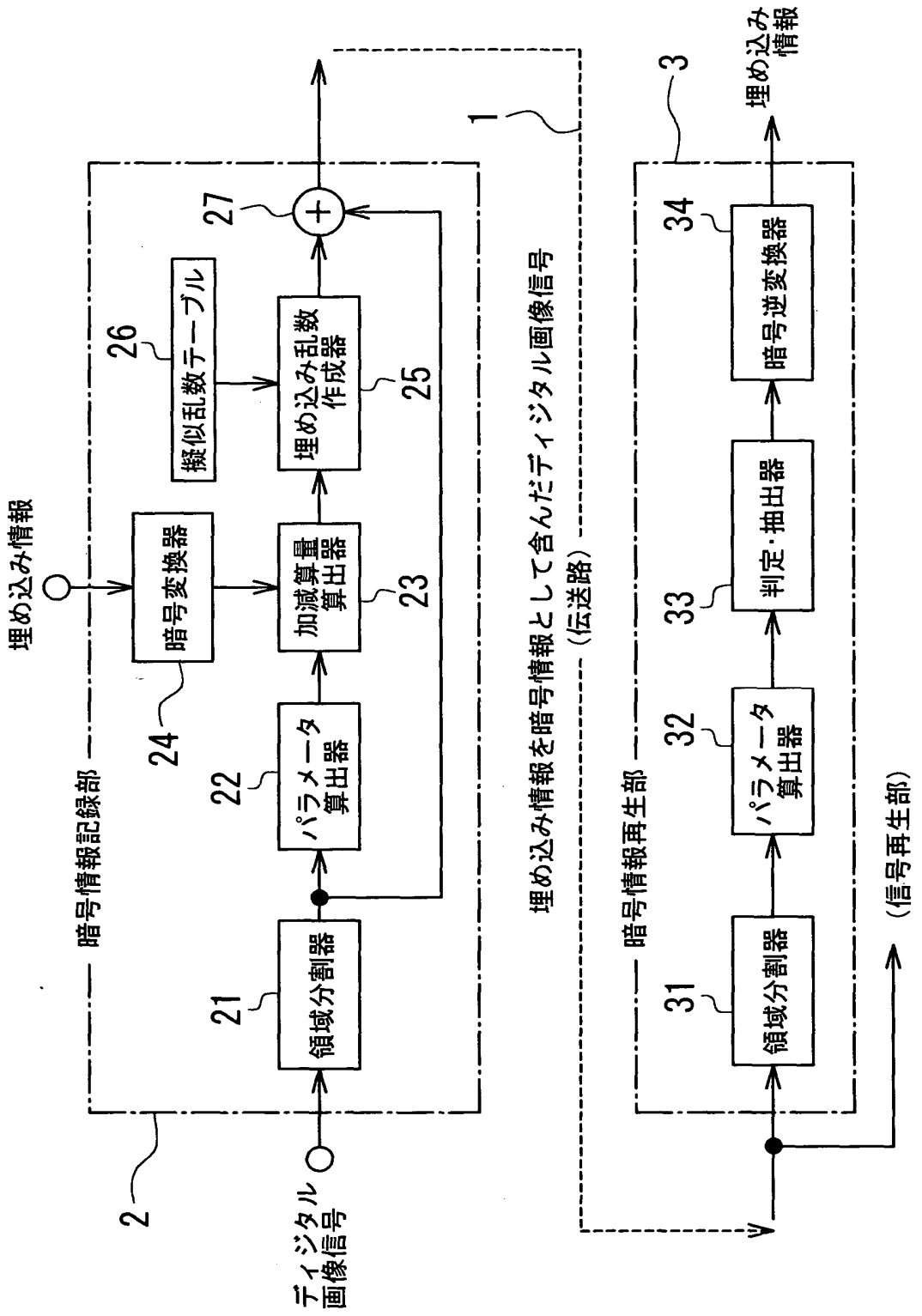
【符号の説明】

１…伝送路、２，2’…暗号情報記録部、３，3’…暗号情報再生部、２１，３１…領域分割器、２２，３２…パラメータ算出器、２３…加減算量算出器、２４

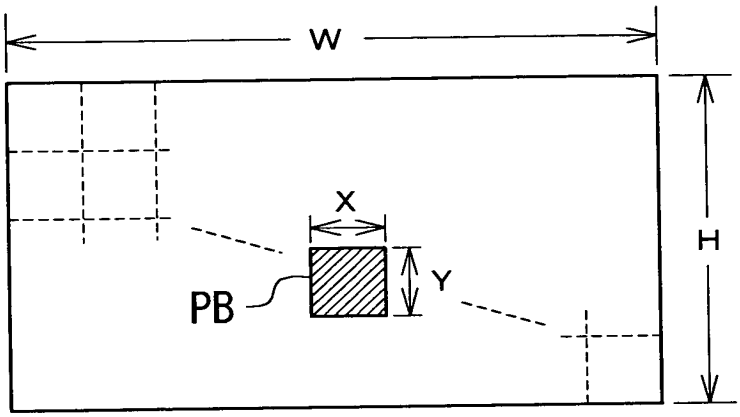
…暗号変換器、２５…埋め込み乱数作成器、２６…擬似乱数テーブル、３３…判定・抽出器、３４…暗号逆変換器、４１，５１…ＲＯＭ、４２，５２…ＣＰＵ、４３，５３…ＲＡＭ、４４，５４…ＲＡＭ。

【書類名】　図面

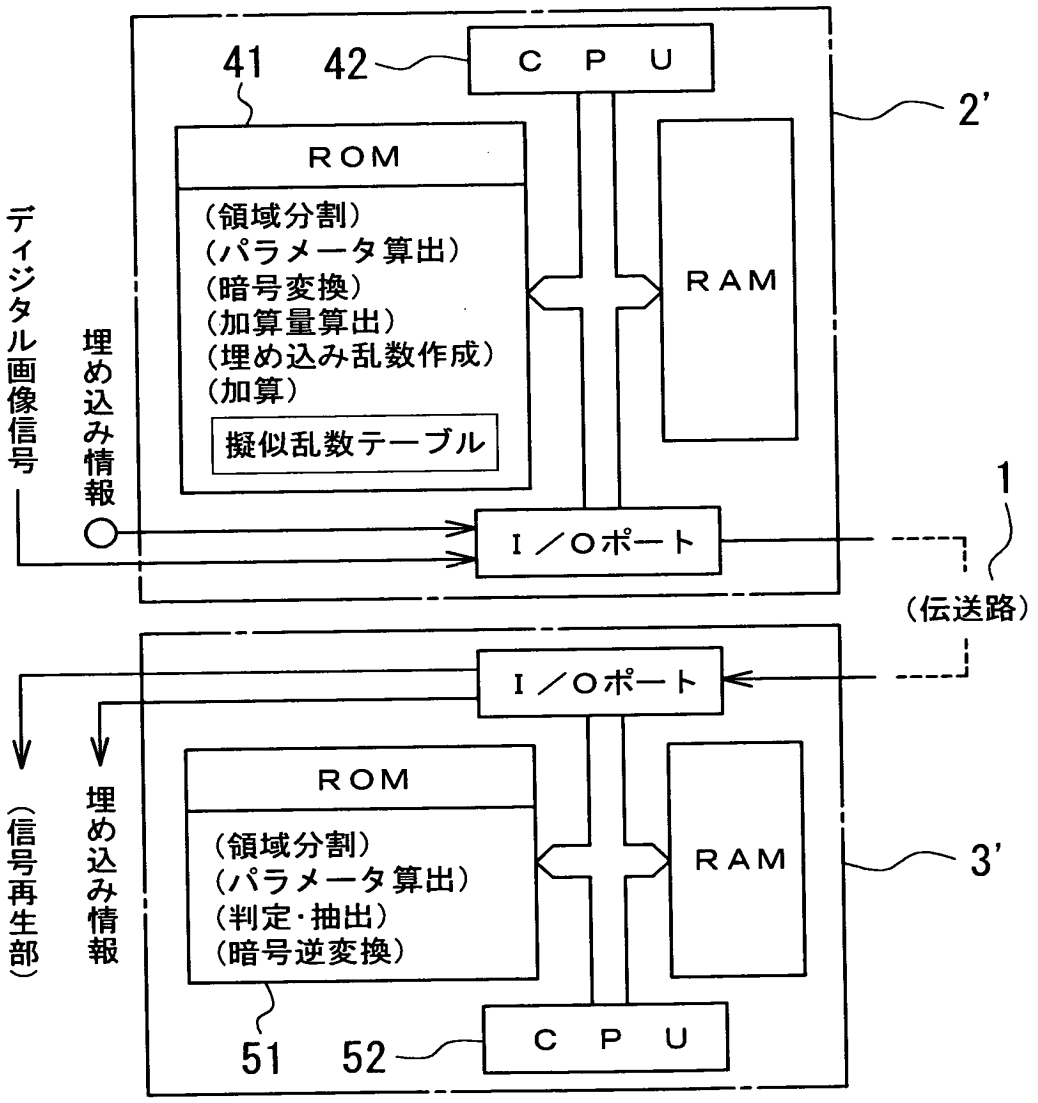
【図１】


埋め込み情報
暗号情報記録部
暗号変換器
24
擬似乱数テーブル
26
27
埋め込み乱数作成器
25
加減算量算出器
23
パラメータ算出器
22
領域分割器
21
2
ディジタル画像信号
1
埋め込み情報を暗号情報として含んだディジタル画像信号
（伝送路）
3
暗号情報再生部
領域分割器
31
パラメータ算出器
32
判定・抽出器
33
暗号逆変換器
34
埋め込み情報
（信号再生部）

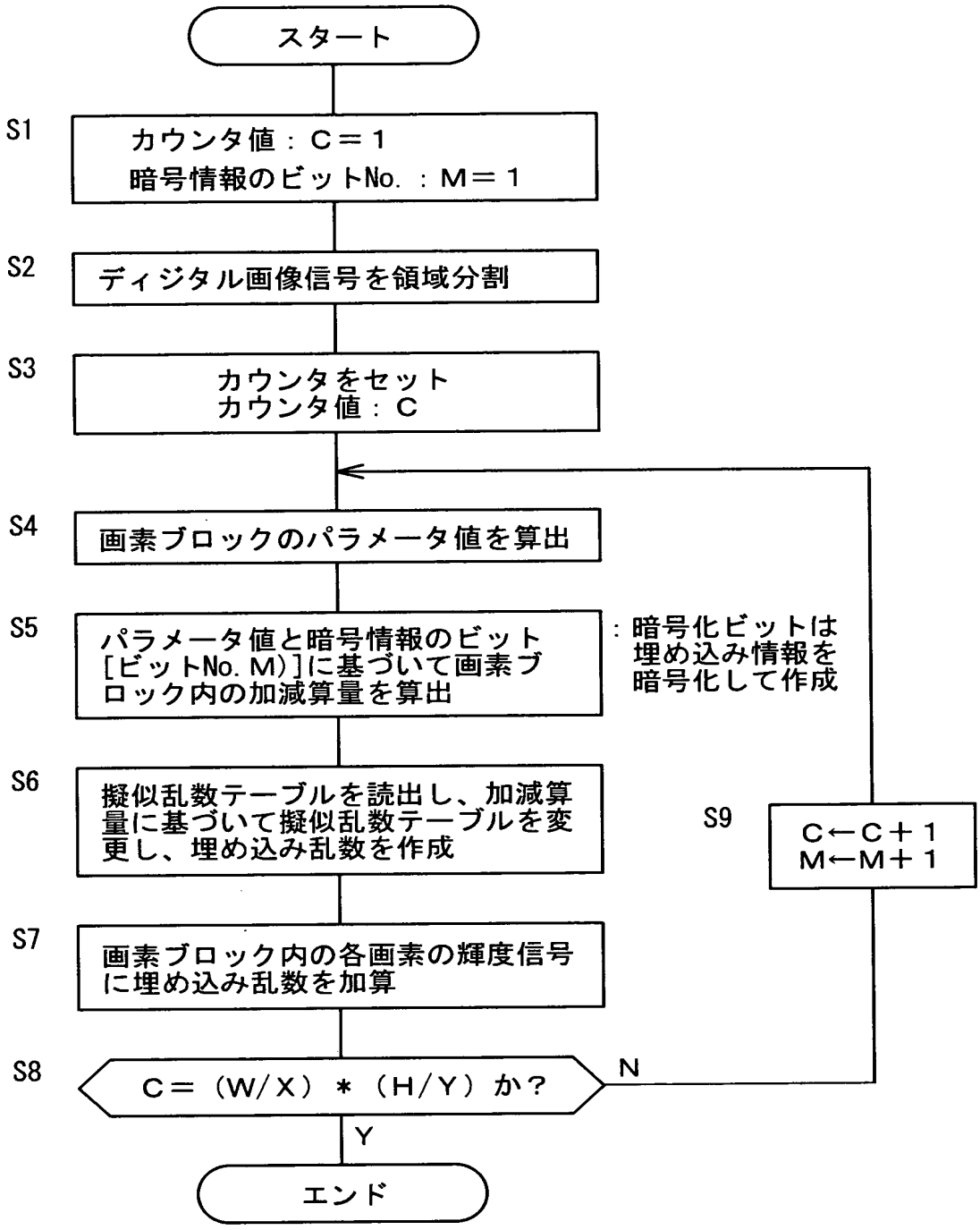
【図２】


W
H
X
Y
PB

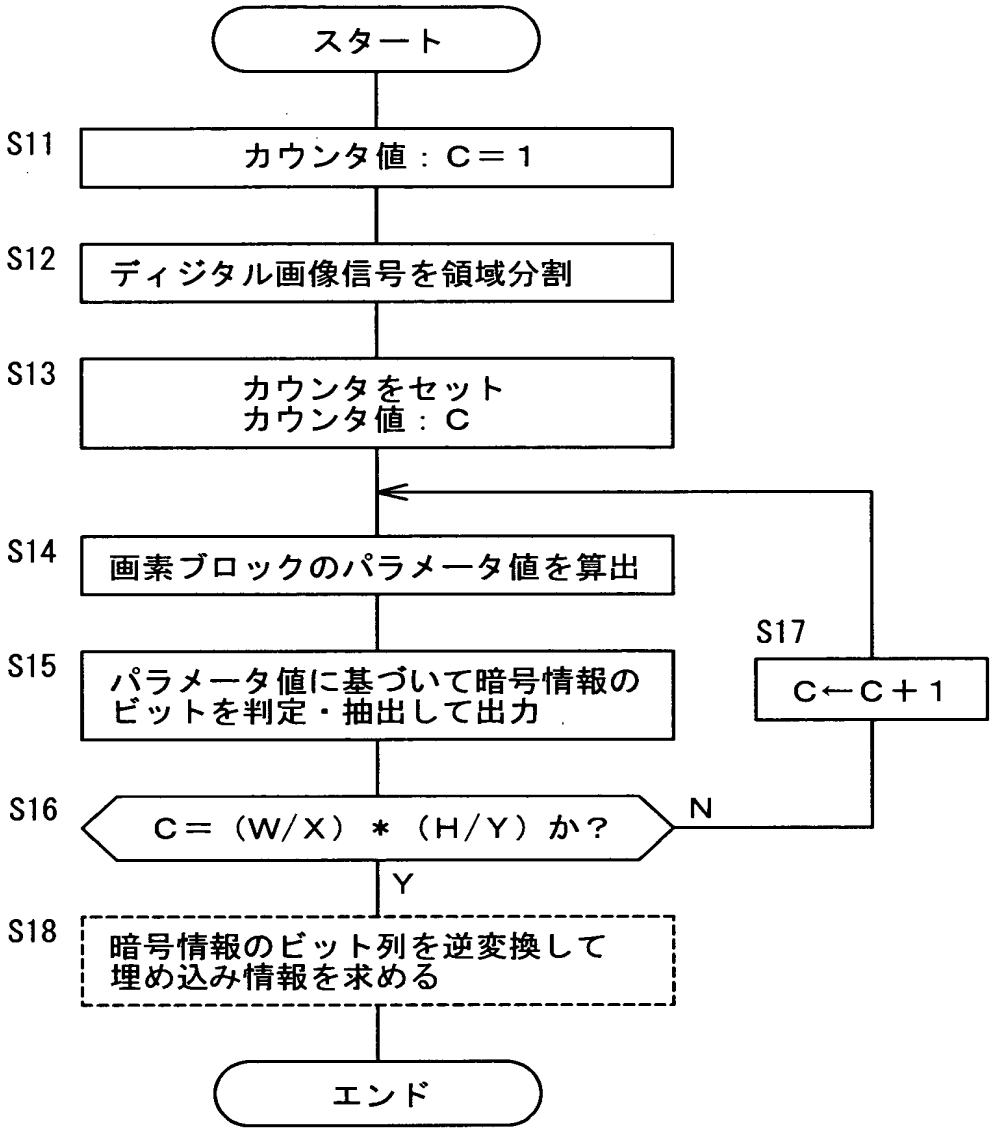
【図３】


41
42
C P U
2'
ROM
(領域分割)
(パラメータ算出)
(暗号変換)
(加算量算出)
(埋め込み乱数作成)
(加算)
擬似乱数テーブル
RAM
ディジタル画像信号
埋め込み情報
I／Oポート
1
(伝送路)
I／Oポート
(信号再生部)
埋め込み情報
ROM
(領域分割)
(パラメータ算出)
(判定・抽出)
(暗号逆変換)
RAM
3'
51
52
C P U

【図４】


スタート
S1
カウンタ値：Ｃ＝１
暗号情報のビットNo.：Ｍ＝１
S2
ディジタル画像信号を領域分割
S3
カウンタをセット
カウンタ値：Ｃ
S4
画素ブロックのパラメータ値を算出
S5
パラメータ値と暗号情報のビット[ビットNo. M)]に基づいて画素ブロック内の加減算量を算出
：暗号化ビットは埋め込み情報を暗号化して作成
S6
擬似乱数テーブルを読出し、加減算量に基づいて擬似乱数テーブルを変更し、埋め込み乱数を作成
S7
画素ブロック内の各画素の輝度信号に埋め込み乱数を加算
S8
Ｃ＝（W/X）＊（H/Y）か？
N
Y
S9
Ｃ←Ｃ＋１
Ｍ←Ｍ＋１
エンド

【図５】


スタート
S11
カウンタ値：Ｃ＝１
S12
ディジタル画像信号を領域分割
S13
カウンタをセット
カウンタ値：Ｃ
S14
画素ブロックのパラメータ値を算出
S15
パラメータ値に基づいて暗号情報の
ビットを判定・抽出して出力
S16
Ｃ＝（Ｗ/Ｘ）＊（Ｈ/Ｙ）か？
N
Y
S17
Ｃ←Ｃ＋１
S18
暗号情報のビット列を逆変換して
埋め込み情報を求める
エンド

【書類名】　　要約書

【要約】

【課題】　ディジタル・コンテンツに対する暗号情報（著作権情報等）の埋め込みとその再生を簡単な装置と手順で実現する。

【解決手段】　暗号情報記録部２では、領域分割部２１でディジタル信号をデータブロックに分割し、パラメータ算出部２２で前記ブロック内の信号の統計量（平均値と総和値）を求め、加減算量算出器２３で統計量と埋め込み情報を暗号化した暗号情報に基づいて統計量を変化させるための加減算量を算出し、埋め込み乱数作成器２５で擬似乱数に加減算量を加算して新たな擬似乱数信号を作成し、加算器２７によって擬似乱数信号を元のブロックの信号に加算する。暗号情報再生部３では、領域分割器３１で伝送信号をブロック単位に分割し、パラメータ算出器３２でブロック内の信号の統計量を求め、判定・抽出器３３で暗号情報を抽出した後、暗号逆変換器３４で埋め込み情報を再生する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　　日本ビクター株式会社